VOLKTEK

NSH-2926/NSH-2916

16-port/ 24-port Managed Gigabit
Web Smart Switch

User Manual

www.volktek.com

COPYRIGHT

FCC WARNING

This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment gene rates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

CAUTION

RISK OF EXPLOSION IF A BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

Take special care to read and understand all the content in the warning boxes:

Table of Contents

About This Guide

Welcome

Congratulations on choosing the NSH-2926 24-port 10/100/1000Base-T + 2-port Gigabit SFP (NSH-2916 16 x 10/100/1000Base-T ports) Web Smart Switch. The NSH-2926(NSH-2916) is a high-performance Web-Smart switch that provides users with 24x10/100/1000Mbps Ethernet and two Gigabit SFP slots (16 x 10/100/1000Base-T ports).The Web/SNMP management provides remote control capability that provides flexible network management and monitoring options. Whether managed via an "in-band" SNMP management station or an Internet Web browser, the NSH-2926(NSH-2916) facilitates network operational control and diagnostics.

The management functions enable efficient network usage. VLAN reduces the collisions caused by broadcasting. QoS secures the bandwidth for some bandwidth-hungry applications like VoIP and video conferencing. The Switch also supports Port Mirroring that allows web manager to watch abnormal traffic.

Purpose

This guide discusses how to install and configure your Web Smart Access Switch.

Terms/ Usage

In this guide, the term “Switch” (first letter upper case) refers to the NSH-2926(NSH-2916) Switch, and “switch” (first letter lower case) refers to other switches.

Features

- NSH-2926 for 24-port 10/100/1000 T plus two fiber ports / NSH-2916 for 16-port 10/100/1000 T
- RSTP
- ARP Inspection
- IGMP Snooping (v1/2/3)
- IGMP Querier
- Loop Detection
- Port-based VLAN
- 802.1Q VLAN 256 Static Maximum
- VLAN trunking
- Guest VLAN
- 802.1x port authentication
- Static MAC forwarding
- Web authentication
- 802.1p QoS with 8 CoS per port
- Diffserv

- Broadcast Storm Control
- Bandwidth Control
- Rate limitation
- 802.3 flow control
- Link aggregation (802.3ad)
- Port-based mirroring
- Web GUI management
- SNMP (v1/v2)
- EEE support

Specifications

Performance:

Throughput:	14,881 packets per second (pps) to 10 Mbps ports 148,809 pps to 100Mbps ports 1,488,095 pps to 1000Mbps ports
Address Table Size:	16K MAC entries
VLANs:	Port-based Tag-based (4096VLANs)
Link Aggregation:	Up to eight aggregation groups
Max. Distance:	UTP: 100 meters
Fiber:	Based on Mini GBIC module
Management via:	SNMP V1, V2C Web Management

Connectors and Cabling:

Ports:	NSH-2926 24 x 10/100/1000Mbps ports 2 x Gigabit fiber slots (SFP) NSH-2916 16 x 10/100/1000Mbps ports

SNMP Standards & Protocols:

RFC 1157	Simple Network Management Protocol v2c
RFC 1213	MIB II
RFC 1493	Bridge MIB
RFC 1643	Ethernet MIB
RFC 1757	RMON Group 1, 2, 3, 9

Network Management:

System Configuration:	Telnet, Web browser, and SNMP/RMON
Management Agent:	SNMP Support: MIB II, Bridge MIB, Ethernet MIB, and RMON MIB
RMON Groups:	1, 2, 3, and 9 (Statistics, History, Alarm and Event)
Spanning Tree Algorithm:	IEEE 802.1D and 802.1w provide redundant link support
Port-based or 802.1Q VLANs:	Up to 4096 VLANs, with GVRP for dynamic VLAN registration
Link Aggregation:	2~8 ports can be combined into a fat pipe

Standards and Compliance:

IEEE 802.3 10Base-T Ethernet
IEEE 802.3u 100Base-TX Ethernet
EEE 802.3ab 1000Base-T Ethernet
IEEE 802.3z 1000Base-SX/LX/LHX
IEEE 802.3 NWay Auto-negotiation
IEEE 802.3x Flow Control
IEEE 802.1D Spanning Tree protocol
IEEE 802.1w Rapid Spanning Tree protocol
IEEE 802.1p Class of Service, Priority protocols
IEEE 802.1Q VLAN Tagging
IEEE 802.1X Port Authentication
IEEE 802.1ad VLAN Stacking
IEEE 802.3ad LACP Aggregation

Power Characteristics:

Input voltage:	100 to 240V AC (auto-ranging) 50 to 60 Hz
Power Consumption:	20-Watts max.

Environmental Characteristics:

Operating	Temperature: 0°C to 50°C Relative Humidity: 10% to 80%, non-condensing
Storage	Temperature: 0°C to 70°C Humidity: 5% to 90% (non-condensing)

Dimensions:

44.5mm (H) x 440mm (W) x 173mm (D)

Weight:

2.3kg

Mounting:

Standard 19" Rack-mountable case

Electromagnetic Compatibility:

Emissions: FCC Class A, & CE approved

Hardware Description

The NSH-2926(NSH-2916) is a high-performance managed SNMP Layer 2+ switch that provides users with 24 x 10/100/1000Mbps Ethernet and two Gigabit Combo ports. The Web/SNMP management provides remote control capability that gives user-friendly and flexible network management and monitoring options.

For increased bandwidth applications, the NSH-2926(NSH-2916) can accommodate trunk groups with eight ports in each trunk, up to eight trunking groups.

Moreover, these trunk ports ship with fair-over function to provide redundant backup if one or more of the ports are malfunctioning. It also supports both Port-based VLAN and Tag-based VLAN, thereby simplifying network traffic segmentation, broadcast domain extension and other associated benefits of constructing VLANs. This abundance of features translates into increased efficiency and performance in network administration.

Being SNMP-ready, the Switch enables network managers to remotely monitor the entire network status quickly and easily via RJ-45 (in-band), or connection. This managed Switch can extend the enterprise LAN configuration range up to 110km while simultaneously minimizing the troubleshooting time. The Switch is designed for 'plug-n-play' to enable hassle-free integration in today's managed mixed cabling network configurations.

Featuring auto MDI/MDI-X detection for direct connections to a workstation, switch or hub, network managers no longer need to worry about the cable configuration (crossover or straight through) when establishing connections between RJ-45 ports.

The Switch has auto-negotiation capabilities that allow it to support connection with leading NWay switches. In full-duplex mode, this unit can sustain distances of up to 550m (with multi-mode fiber) and 110km (with long-haul single-mode fiber) between a LAN switch and another switch or data/file server.

Product Illustration

NSH-2926

Front View:

Back View

NSH-2916

Front View

Back View

Connectors

The Switch NSH-2926 utilizes ports with copper and SFP fiber port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

The Switch NSH-2916 utilizes ports with copper port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

10/100/1000Base-T Ports

The 10/100/1000BASE-T ports support network speeds of either 10Mbps, 100Mbps, or 1000Mbps and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true "plug-n-play" capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are recommended cabling for the RJ-45 connectors: (1)10Mbps – Cat 3 or better; (2)100Mbps – Cat 5e or better; (3) 1000Mbps – Cat 5e or better.

SFP Slots for SFP modules (For NSH-2926 only)

The two SFP slots are designed to house Gigabit SFP modules that support network speeds of 1000Mbps.

Installation

The location chosen for installing the Switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- Leave at least 10cm of space at the front and rear of the unit for ventilation.
- Affix the provided rubber pads to the bottom of the Switch to protect the case from scratching.

Desktop Installation

Follow the instructions listed below to install the Switch in a desktop location.

1. Locate the Switch in a clean, flat and safe position that has convenient access to AC power.
2. Affix the four self-adhesive rubber pads to the underside of the Switch.
3. Apply AC power to the Switch (The green PWR LED on the front panel should light up).
4. Connect cables from the network partner devices to the ports on the front panel (The green LNK LED on the upper right of the port should light).

This Switch can also be mounted on a vertical surface. Simply use the underside of the unit as a template to measure and mark out the position of the holes on to the surface where the unit is to be installed. Then use the two screws provided to mount the Switch firmly in place.

> **Warning:** Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

Mounting on a Rack

Attach brackets to each side of the switch and place the brackets in the rack's slots.
Insert and tighten two screws to securely attach the bracket to the rack on each side.

Getting Connected

The Switch is capable of connecting up to 26 network devices employing a combination of twisted-pair and fiber cabling paths at Ethernet, Fast Ethernet, or Gigabit Ethernet speeds.

Powering On the Unit

The Switch uses an AC power supply 100~240V AC, 50~60 Hz. The Switch's power supply automatically self-adjusts to the local power source and may be powered on without having any or all LAN segment cables connected.

1. Insert the power cable plug directly into the receptacle located at the back of the device.
2. Plug the power adapter into an available socket.
Note:*For international use, you may need to change the AC power adapter cord. You must use a power cord set that has been approved for the receptacle type and electrical current in your country.*
3. Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

Installing the SFP modules and Fiber Cable (For NSH-2926 only)

1. Slide the selected SFP module into the selected SFP slot. (Make sure the SFP module is aligned correctly with the inside of the slot):

2. Remove any rubber plugs that may be present in the SFP module's mouth.

3. Align the fiber cable's connector with the SFP module's mouth and insert the connector:

4. Slide the connector in until a click is heard:

5. If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.

To properly connect fiber cabling: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Note: When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Check the corresponding port LED on the Switch to be sure that the connection is valid. (Refer to the LED chart)

Connecting a Copper Cable

The 10/100/1000BASE-T RJ-45 Ethernet port fully supports auto-sensing and auto-negotiation.

Insert one end of a Category 3/4/5/5e (see recommendation above) type twisted-pair cable into an available RJ-45 port on the Switch and the other end into the port of the network node.

Check the corresponding port LED on the Switch to ensure that the connection is valid. (Refer to LED chart)

Connecting to Computers or a LAN

You can use Ethernet cable to connect computers directly to the switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either the crossover or straight-through Ethernet cable to connect computers, hubs, or switches.

Use a twisted-pair Category 5 Ethernet cable to connect the 1000BASE-T port, otherwise the link speed will not be able to reach 1Gbps.

Power On the Unit

Connect the AC power cord to the POWER receptacle on the front of the Switch and plug the other end of the power cord into a wall outlet or a power strip.

Check the front LED indicators with the description in the next chapter. If the LEDs light up as described, the Switch's hardware is working properly.

LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

Unit LEDs		
LED	Condition	Status
POST	Green On	Self test passes or System is ready
	Flashing	Switch is booting
	Light Off	Self test fails or no power
PWR	Green On	Primary power is normal
	Light Off	Primary power off or failure
SFP LEDs (for NSH-2926 only)		
LED	Condition	Status
Link/Act (25th~26th Ports)	Green On	The port is linked.
	Flashing	Data traffic transmitting
	Light Off	No valid link established on port
Copper Port LEDs		
LED	Condition	Status
LNK/ACT (1st~24th Ports)	Green On	The port is linked.
	Flashing	Data traffic transmitting at 10/1000 Mbps
	Amber on	Data traffic transmitting at 100Mbps
	Light Off	No valid link established on port
FDX	Amber on	Full Duplex
	Off	Half Duplex

Management Options

This system may be managed using web-based management, accessible through a Web browser. This will allow a network administrator to quickly and efficiently set up a network for a small or medium business with a minimum of hassle.

In order to aid discovery of the device on a network by a management PC, VOLKTEK includes a utility to scan the network. The program, called auto_discovery.exe, is available on the CD which accompanies the Switch. To use the program, first install it on a Windows XP/Vista/7 PC, then click to run.

The device discovery screen allows the user to search for a particular switch, or to leave the box blank in order to scan the network for all switches. After clicking **search**, the program will list the switches on the network fitting the model name entered (or all switches, if no model name was entered).

Once the list has been populated, the user can filter to narrow down the number of devices in the list using the filter function.

When the correct switch had been located, double click anywhere on the table row containing the desired switch to open the GUI in your web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a Web browser.

SNMP-based Management

You can manage the Switch with SNMP Manager software. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast/Multicast Storm.

MIBs

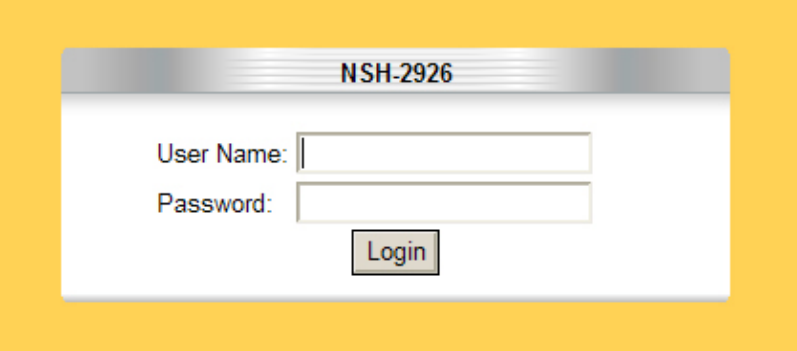
The Switch in the MIB stores management and counter information. It uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. MIB values can be either read-only or read-and-write.

Web Management

The Web Configurator is a browser-based user-friendly interface to allow the network administrator to alter the configuration of the switch. The **Smart** functions are presented on login, with advanced options available through the **Advanced** tab.

Log into Web Management

From a PC, open your Web browser, type the following in the Web address (or location) box: **http://192.168.0.254** and then press **<Enter>**.
This is the factory default IP address for the switch. A login dialog is displayed:



Enter your user name and password, then click Login.
Use the following defaults the first time you log into the program:

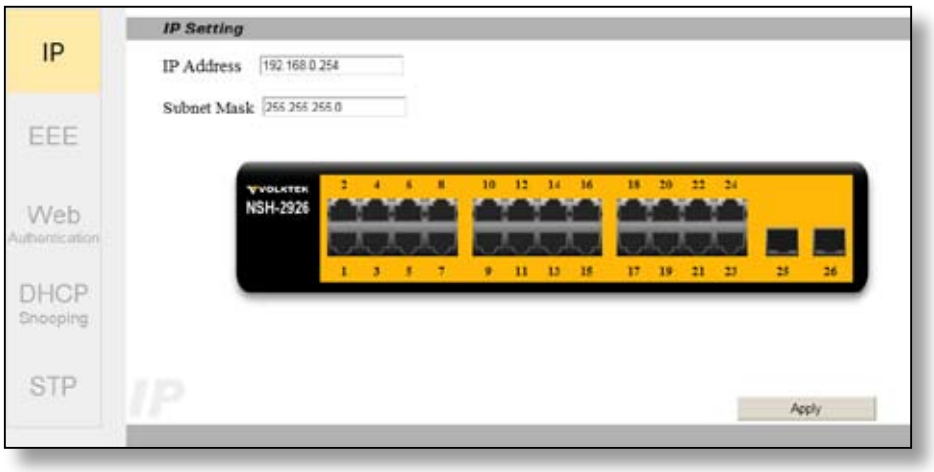
Default User Name: **admin**
Default Password: **admin**

Smart

The Smart tab allows for simple settings, with many of the more advanced features set automatically by the switch.

IP Setting

This function allows the setting of the IP address and subnet mask used by the switch. Enter the desired IP address and subnet mask in the input boxes, then click **Apply** to confirm.

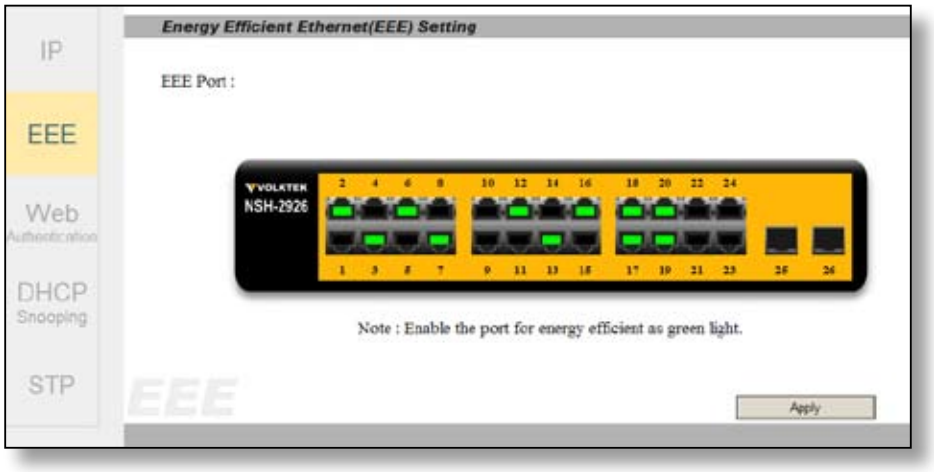


EEE (Energy Efficient Ethernet Port)

The switch is equipped with Energy Efficient Ethernet to reduce energy consumption on Ethernet ports. It is enabled by default.

To disable EEE on all ports, click the **on/off** button.

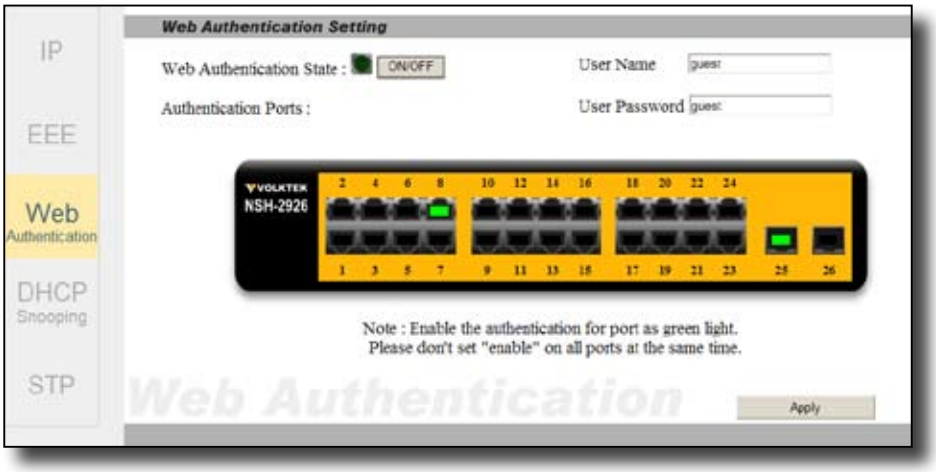
To disable EEE on a per-port basis, click the individual port to be disabled. A green light means EEE is enabled, no light means it is disabled. Once the appropriate ports have been selected, click **Apply**.



Web Authentication

Web authentication allows the admin to set a username and password for logins on a particular port. This is usually employed one guest terminals or networks, for example in a company meeting room, where guests can be allowed to connect to the internet, but not to the local network (which is thereby kept secure). When a device using that port attempts to connect to the internet, the web browser will request a username and password before allowing access.

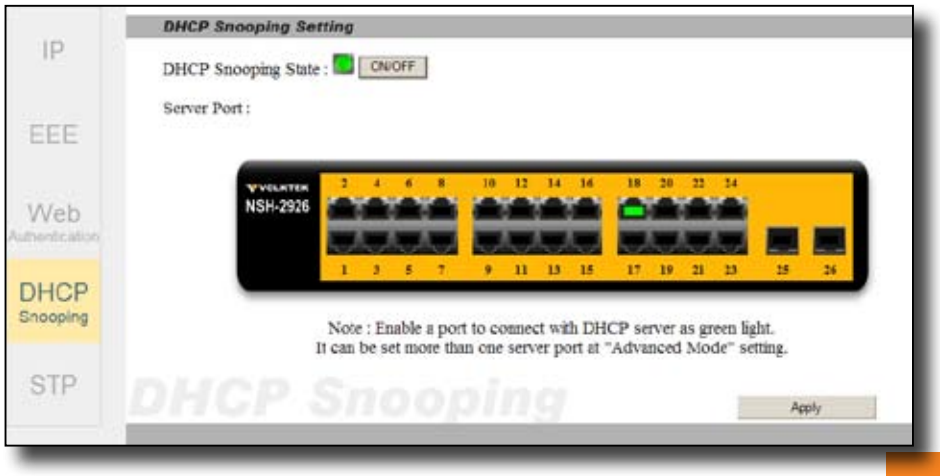
Use the **on/off** button to enable or disable the function. Edit the username and password inputs, click the ports on which web authentication will be enabled (green is enabled, black disabled), then click **Apply** to save.



DHCP Snooping

DHCP snooping is a function which ensures IP integrity in the Layer 2 domain. It listens to network traffic to make sure only authorized devices are accessing the network.

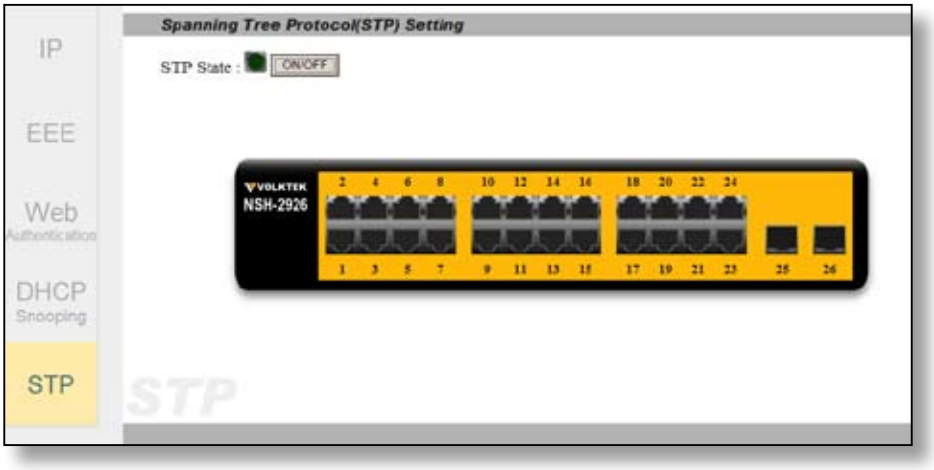
To turn the function for all ports on or off, click the **on/off** button. To allow a particular port to connect with a DHCP server, click the port itself. A green light indicates the port is allowed to connect with a DHCP server, no light means it cannot.



STP (Spanning Tree Protocol)

Spanning Tree Protocol is a network protocol which prevents network loops (which in turn can cause broadcast storm conditions, seriously downgrading network performance).

Click the **on/off** button to enable Spanning Tree Protocol.

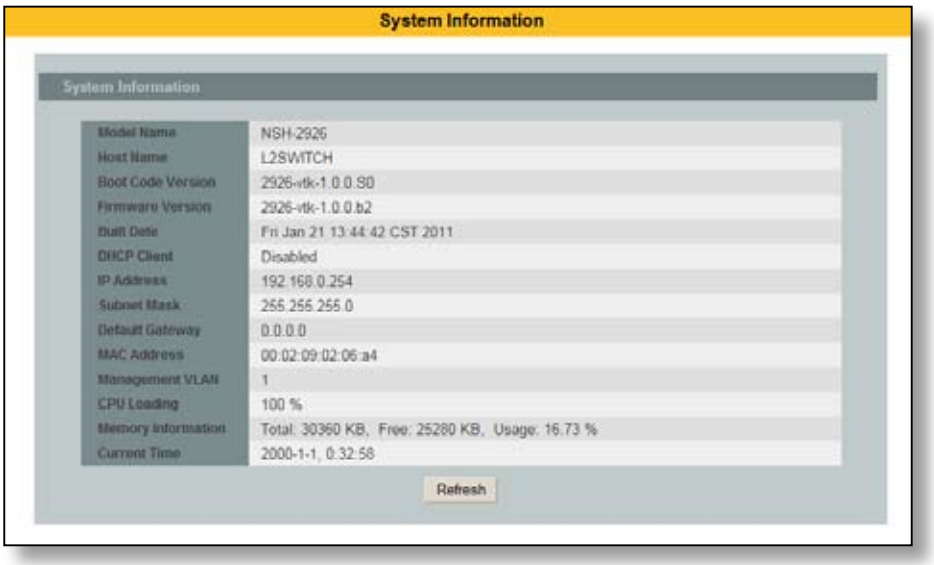


Advanced

The advanced settings tab allows full access to the administrator settings for the switch.

System Status

The system status screen provides information on the current status of the switch.



Basic Settings

The basic settings for the switch are controlled from the **Basic Settings** option.

General Settings

The **System** tab allows access to the **General Settings** window, which contains the following information:
Hostname: Name of the Switch (user editable, no spaces allowed)

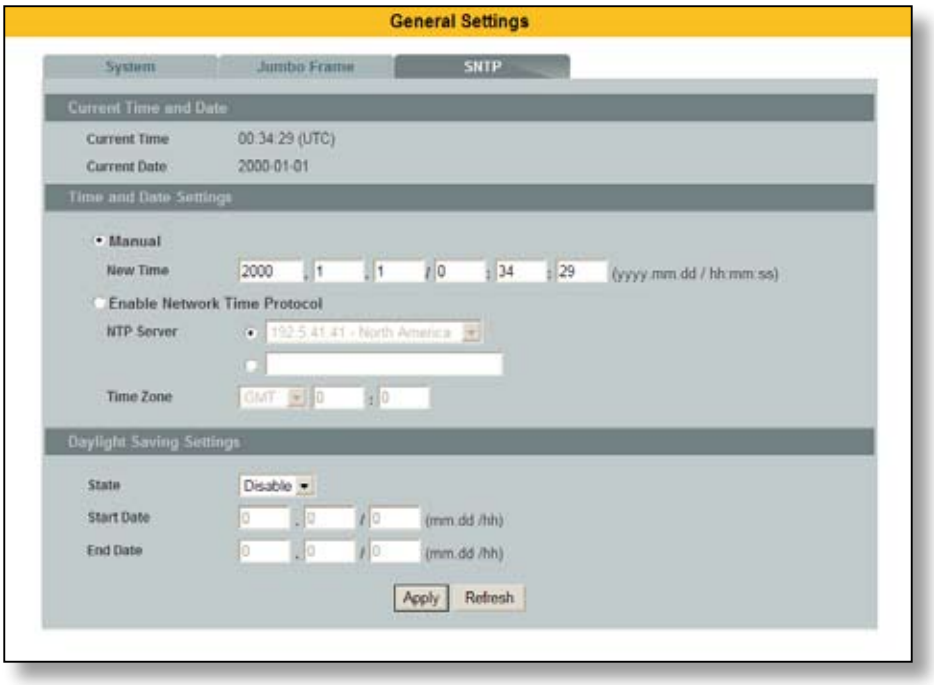
- DHCP Client: Options to enable or disable the DHCP client function of the Switch
- Static IP Address: The IP address of the Switch
- Subnet Mask: The subnet mask for the Switch network
- Default Gateway: The default IP gateway used by the Switch
- Management VLAN: The specific VLAN used for management of the Switch itself

SNTP

The SNTP tab is used for settings related to system time.

In Time and Date Setup the user can manually set the system time and date, or use an NTP client to automatically set the system time and date (recommended).

If manual time and date is enabled, there is an option to set Daylight Savings to adjust the system time on a predetermined date. Select the time adjustment required from the drop-down list, enter the start and finish of the period of daylight savings, then click **Apply** to save these settings.



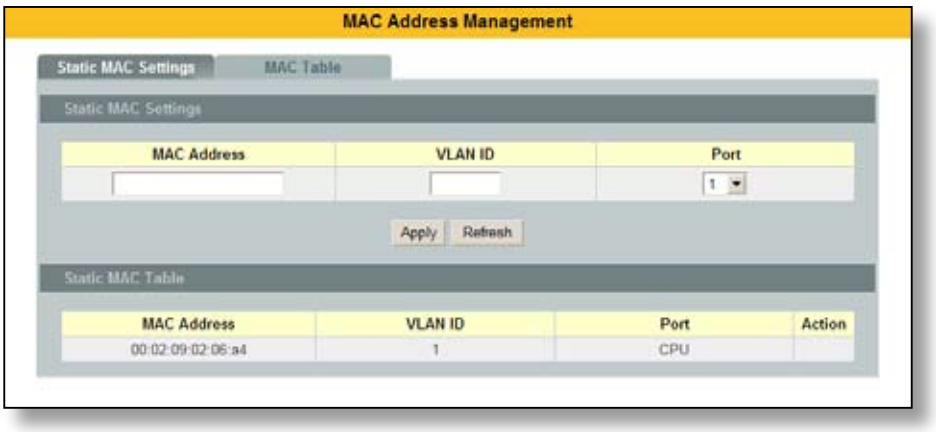
MAC Management

MAC Management can be used to restrict access to certain ports to a specific device by using that device's MAC address. There are two options within the MAC Management setting: Static MAC Settings and MAC Table.

Static MAC Settings is used to assign devices to a particular port. To add a device to the list of permitted devices (the Static MAC Table), enter the MAC Address in the box provided, followed by the relevant VLAN ID and the port number. Click **Apply** to add this device to the Static MAC Table.

Devices can also be deleted from the Static MAC Table by clicking the **Delete** button by the relevant device.

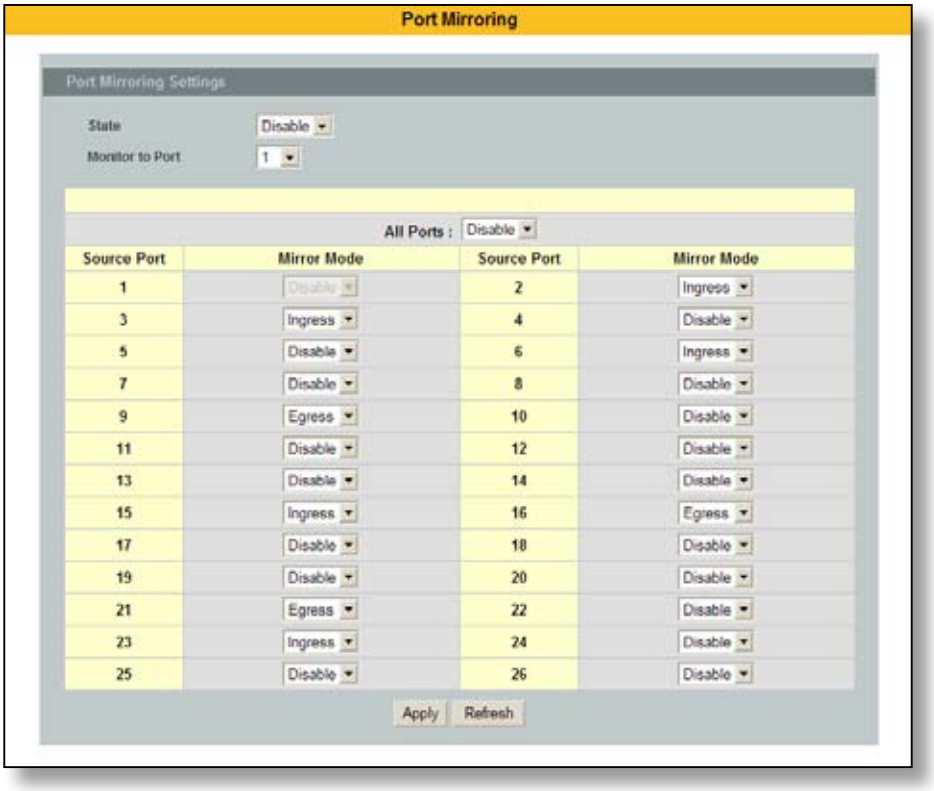
The MAC Table tab allows the network administrator to see the MAC Addresses currently enabled, showing both static and dynamic settings.



Port Mirroring

Port Mirroring will set up a mirror port to send duplicates of each network packet received and/or sent by the original port being mirrored.

To enable, select the source port, the mirror state: **ingress**, i.e. mirror packets coming into the port, **egress**, i.e. packets leaving the port, **both** to select both ingress and egress, and disable to **disable** the function for that particular port.



Port Settings

The port settings menu allows the network administrator to control the settings on individual ports, by selecting from drop-down option lists.

Select the port number, whether to enable or disable settings for that port, the port speed, and flow control.

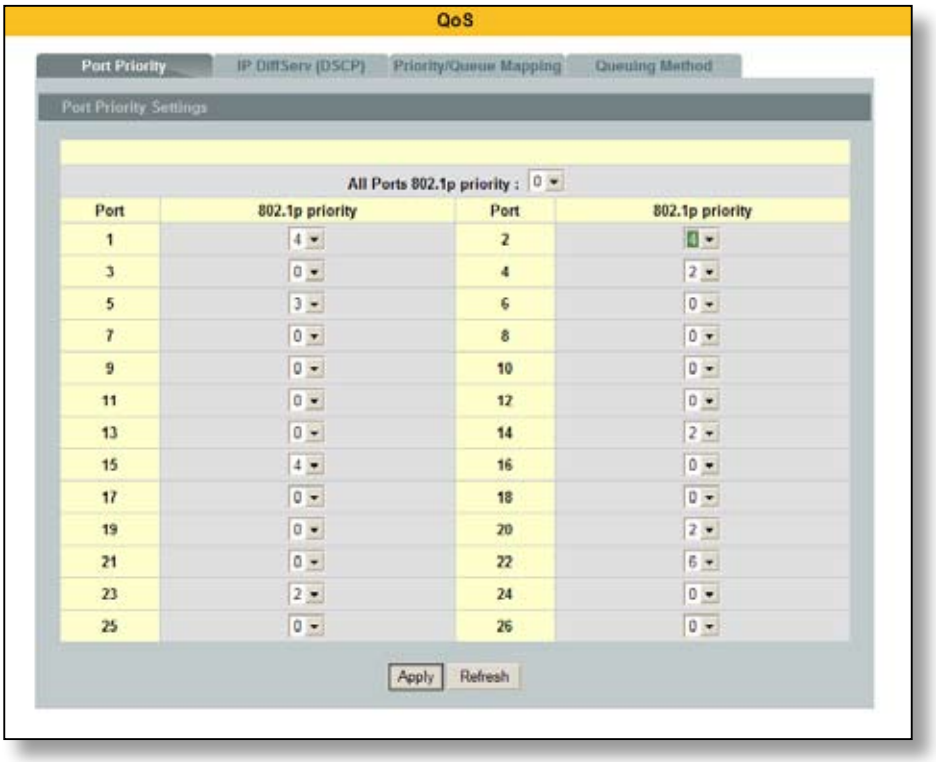
Advanced Settings

The advanced settings menu covers higher-level options for “power administrators”.

Bandwidth Management

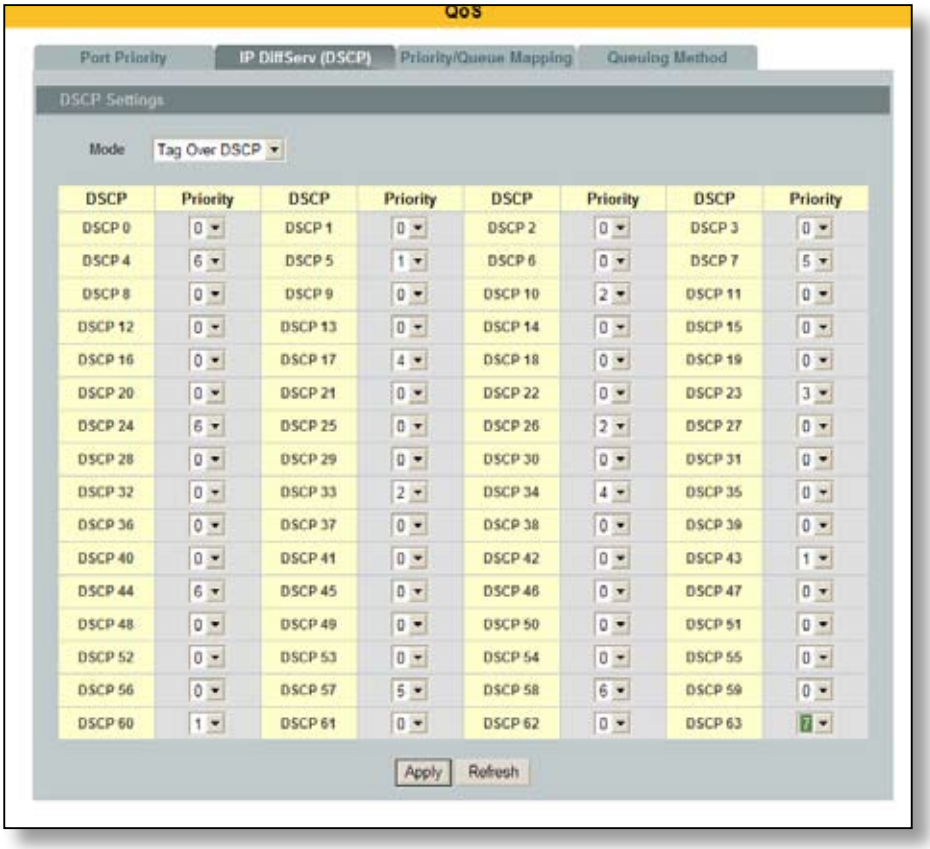
QoS

QoS (Quality of Service) consists of four tabbed options.
Port priority allows the administrator to prioritize certain ports. The higher the number selected, the higher the port priority

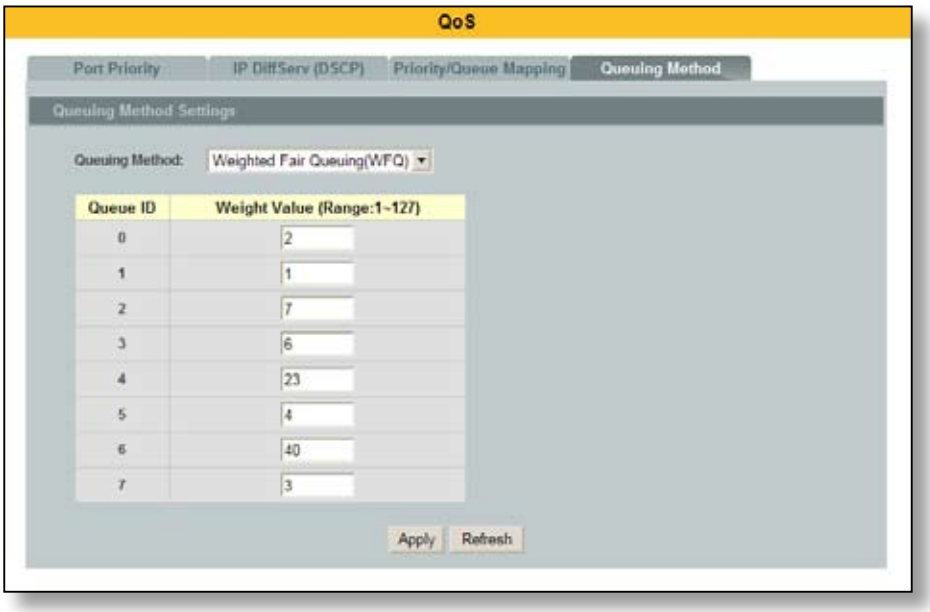


The Diffserv (DSCP) tab allows the prioritization of traffic based on Tag over DSCP (i.e. tagged VLANS have priority over DSCP Diffserv rankings) or DSCP over Tag (i.e. DSCP Diffserv rankings have priority over tagged VLANs).

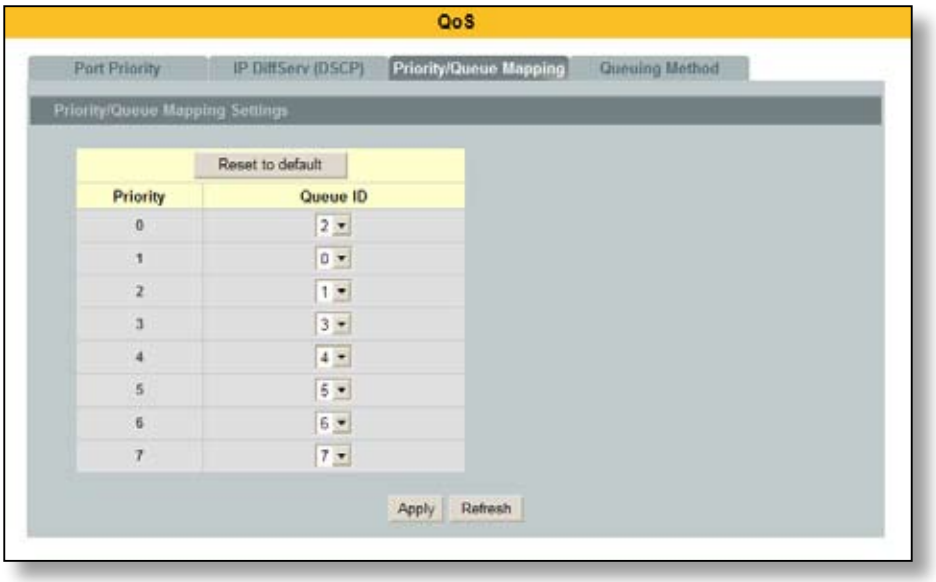
The Priority drop-down menu by each DSCP entry should be set to the desired value, with 0 having no priority, and 7 the highest priority.



The **Queueing Method** tab determines whether QoS uses the Weighted Fair Queue method or the Weighted Round Robin method, along with the weights assigned to each Queue ID.



CoS Queue Mapping allows the administrator map a certain priority to a certain Queue ID. Select the Queue ID from the drop-down list and click **apply** to save the settings.



Storm Control

Storm control is designed to prevent broadcast storm conditions impairing traffic or crashing the switch. For each port the administrator can set the rate (over which the storm control conditions will be triggered) and the type of action to be taken once that rate is reached, choosing one of the following options:

- Broadcast
- Multicast
- DLF
- Bcast+Mcast (Broadcast and Multicast)
- Mcast+DLF (Multicast and DLF)
- Bcast+DLF (Broadcast and DLF)
- Bcast+Mcast+DLF (Broadcast, Multicast, and DLF)

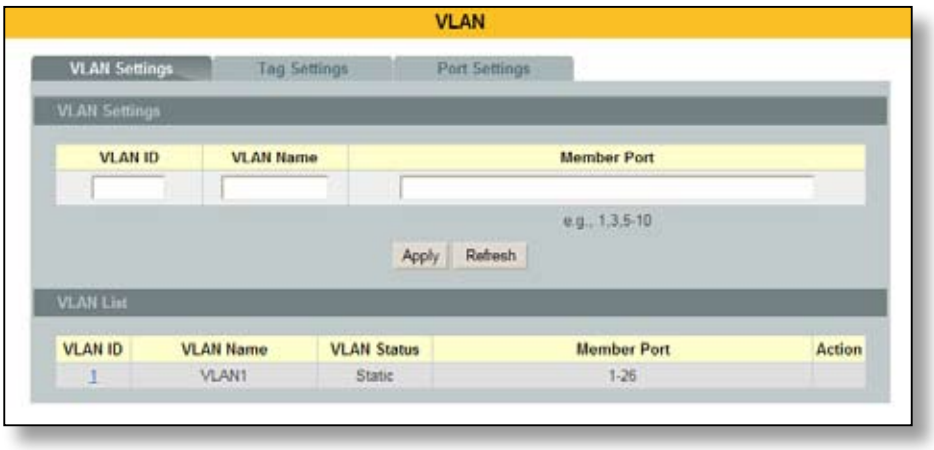
IGMP Snooping

IGMP snooping is a function which allows the switch to "listen in" on layer 3 IGMP packets in a multicast network. It is designed to prevent local hosts from receiving traffic from multicast groups they do not belong to, thereby simplifying network traffic and reducing bandwidth load. The General Settings tab of the IGMP Snooping option allows the administrator to enable or disable the function. The administrator can select on which VLANs to allow IGMP Snooping, and what to do with unknown multicast packets that it discovers (drop or flood).

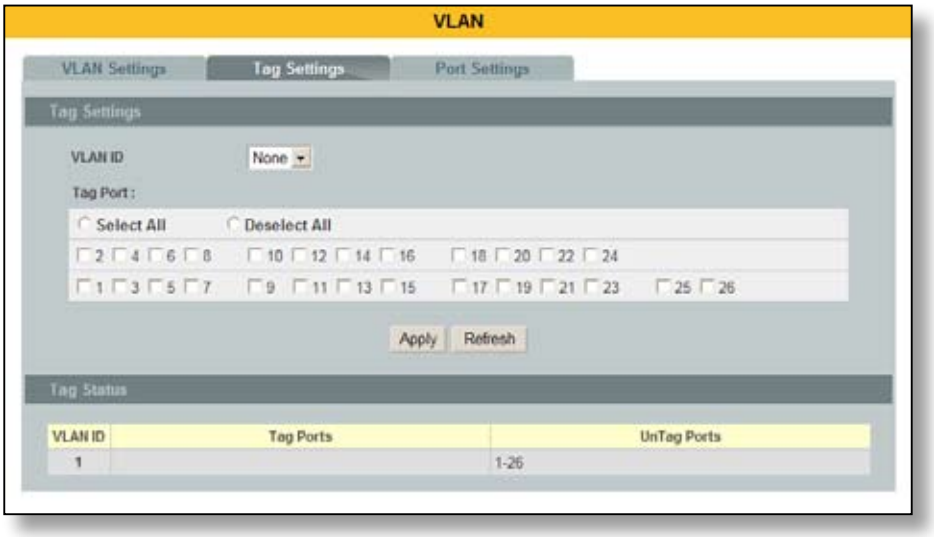
VLAN

A VLAN is a Virtual Local Area Network – a local network which is created using software rather than hardware – meaning that the devices linked by the network need not be physically close to each other. This is useful for determining security and management settings for a group of computers with similar functions (for example, all computers used by clerical staff from different departments in the same company). The VLAN window allows the administrator to configure VLAN options.

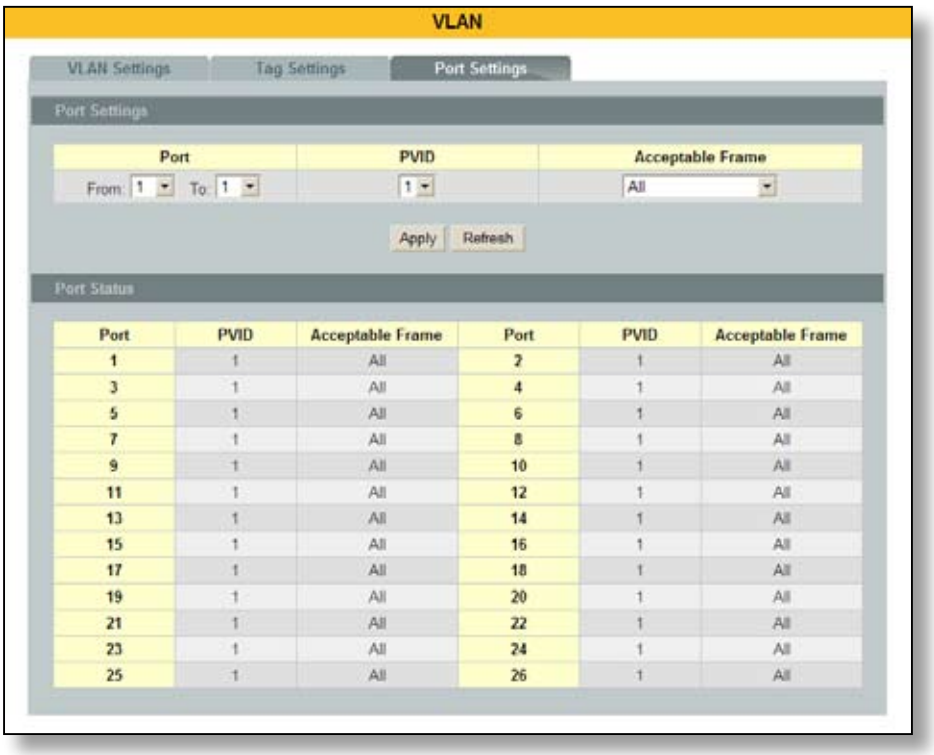
The **member setting** allows the network administrator to assign a particular VLAN ID and name to particular ports. Enter the relevant information and click apply to save.



The **tag setting** option allows the network administrator to select which ports will apply tagging to VLAN packets. Select the relevant ports to be tagged, then click apply to save.



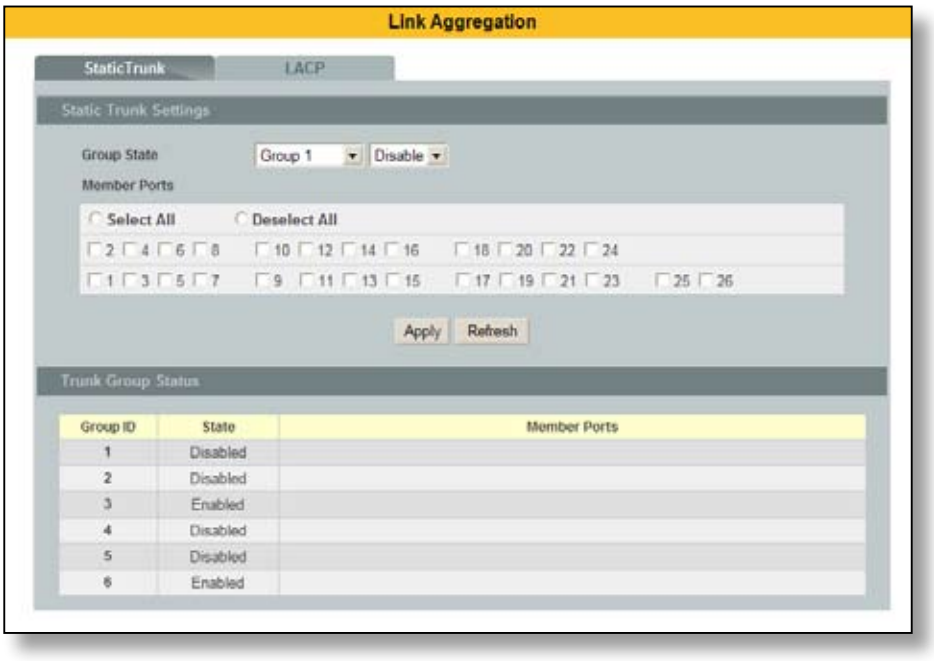
The port setting option allows the network administrator to configure the Port VLAN ID (PVID) for each of the switch ports by selecting the port number, PVID and the type of frames to be accepted by each port.



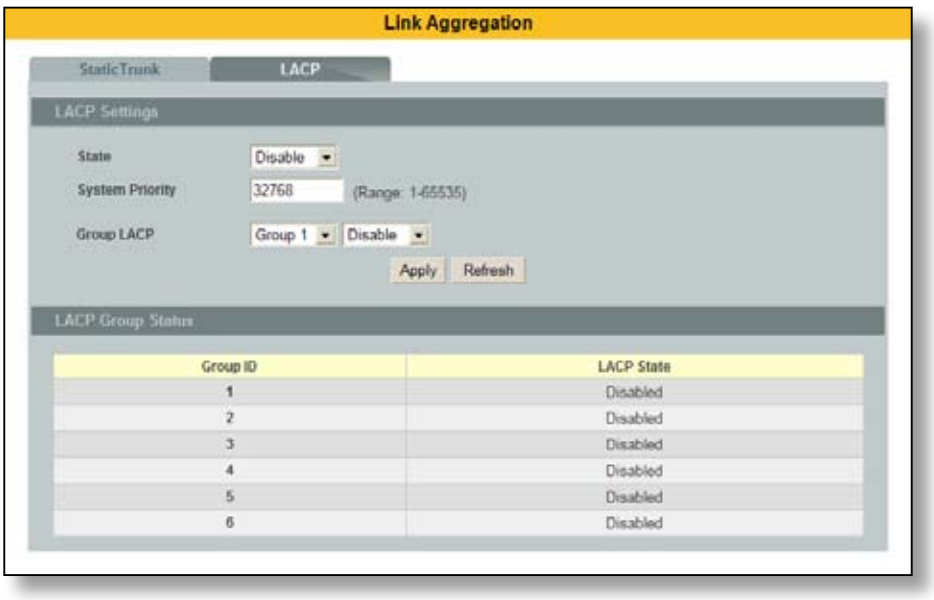
Link Aggregation

Link aggregation allows the network administrator to group ports together to form a virtual “fat pipe”, allowing higher data speeds.

To enable Static Trunk LACP, select the group, group action, and the member ports. Finally, select the load-balancing method, and click **apply** to save.



The network administrator can also control the 802.3ad (global LACP) settings for the switch. Select enable to enable 802.3ad LACP, then enter the group priority order. Click **apply** to save.

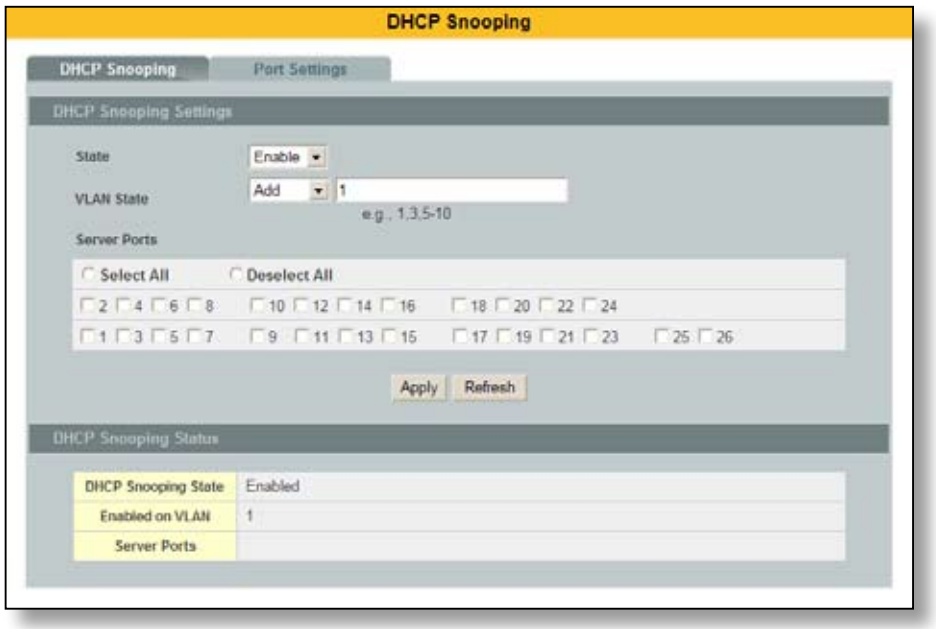


Security

DHCP Snooping

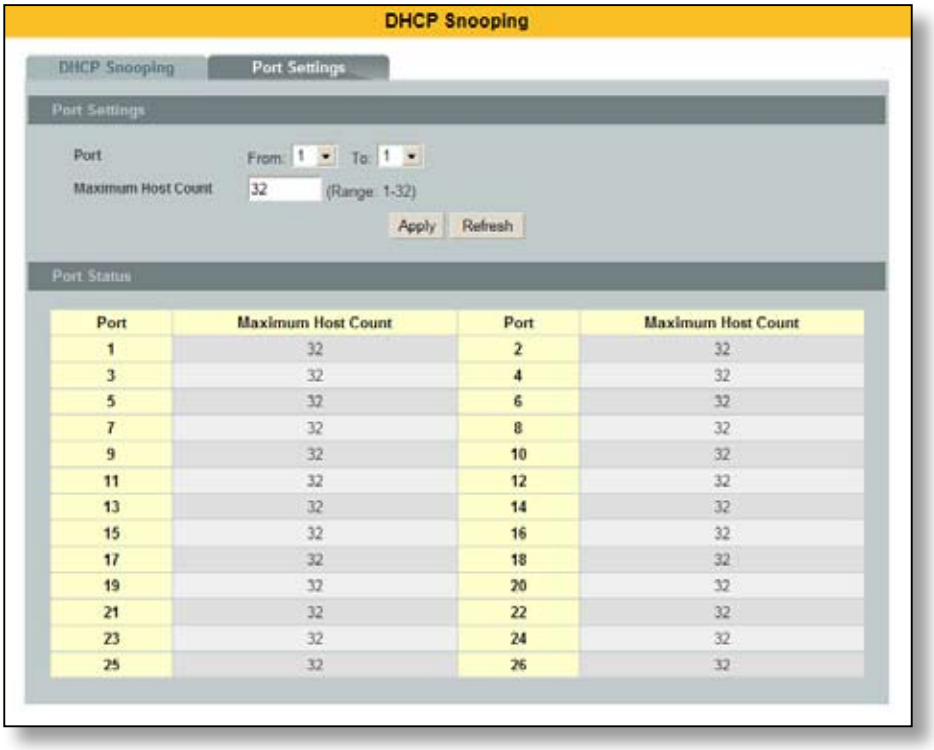
DHCP Snooping checks on incoming traffic and can be set up to allow only certain numbers of users to connect to the switch.

Set the state (enable/disable) and VLAN state (per VLAN enable/disable), then select which ports are to be used as server ports by clicking the radio buttons next to each relevant port number. Click **apply** to save.



The DHCP Snooping Status section shows the currently enabled DHCP snooping details.

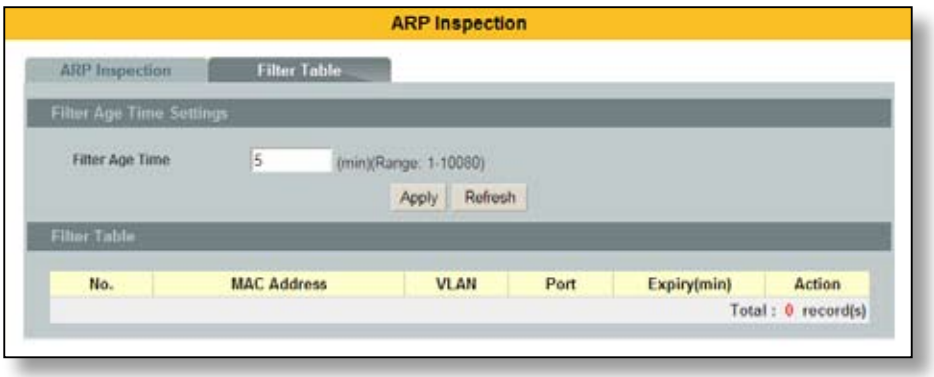
DHCP Port settings allows the network administrator to configure the maximum host count on each port – limiting the number of hosts which can connect to a given host at any time. Select the port required, then enter the maximum host count to be applied. Click **apply** to save.



ARP Inspection

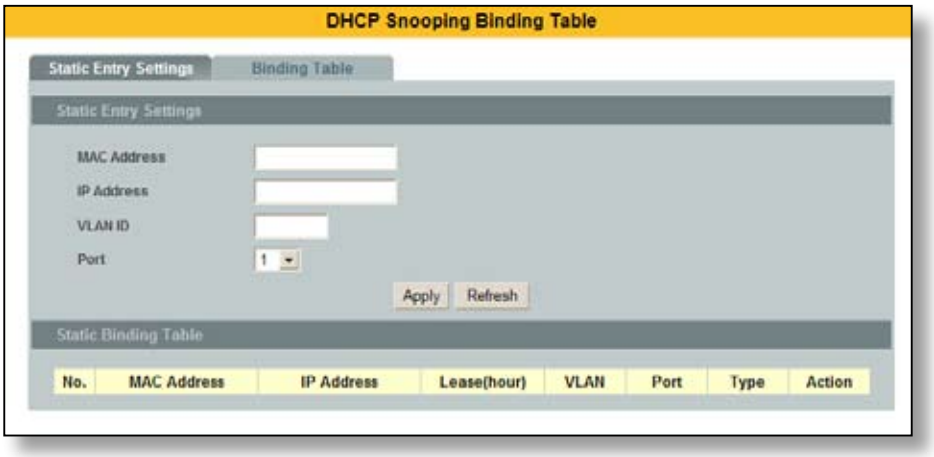
ARP inspection allows the switch to intercept and inspect ARP packets and reroute those packets to specific VLANs as specified in the options.

The ARP filter allows the administrator to inspect the current ARP filter rules in place, and to delete unneeded filters.



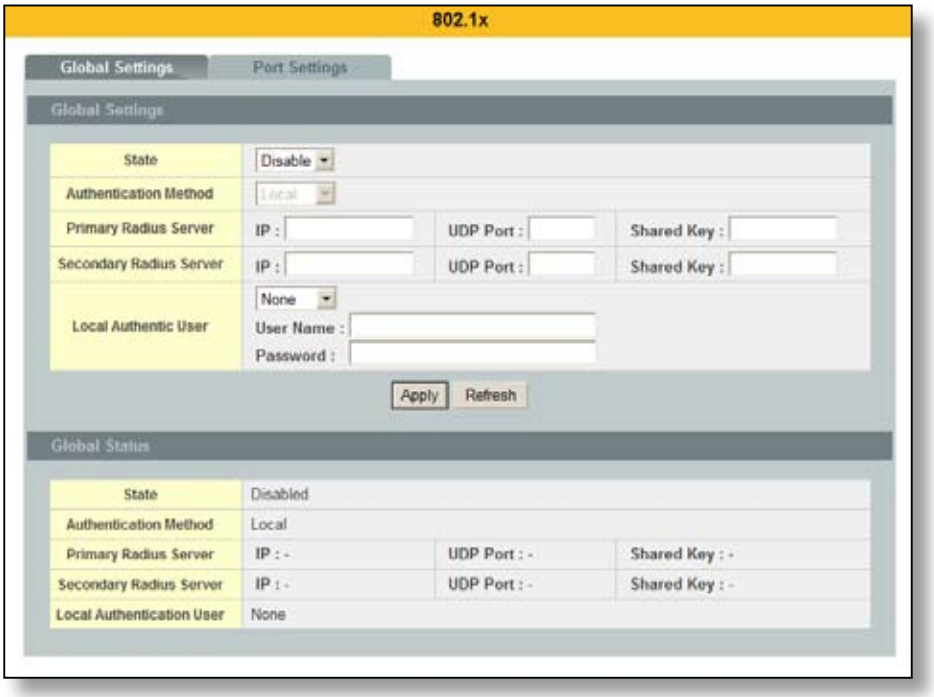
Binding Table

The binding table displays the values used by the ARP inspection protocol. MAC and IP addresses must match the port for the traffic to be allowed. This helps to prevent unauthorised users from connecting to the network.



802.1x

802.1x port authentication is a protocol for authenticating traffic on certain ports. The administrator can choose to enable or disable the function, choose Local or RADIUS as the authentication method, then set the IP, UDP port and Shared Key for RADIUS servers.



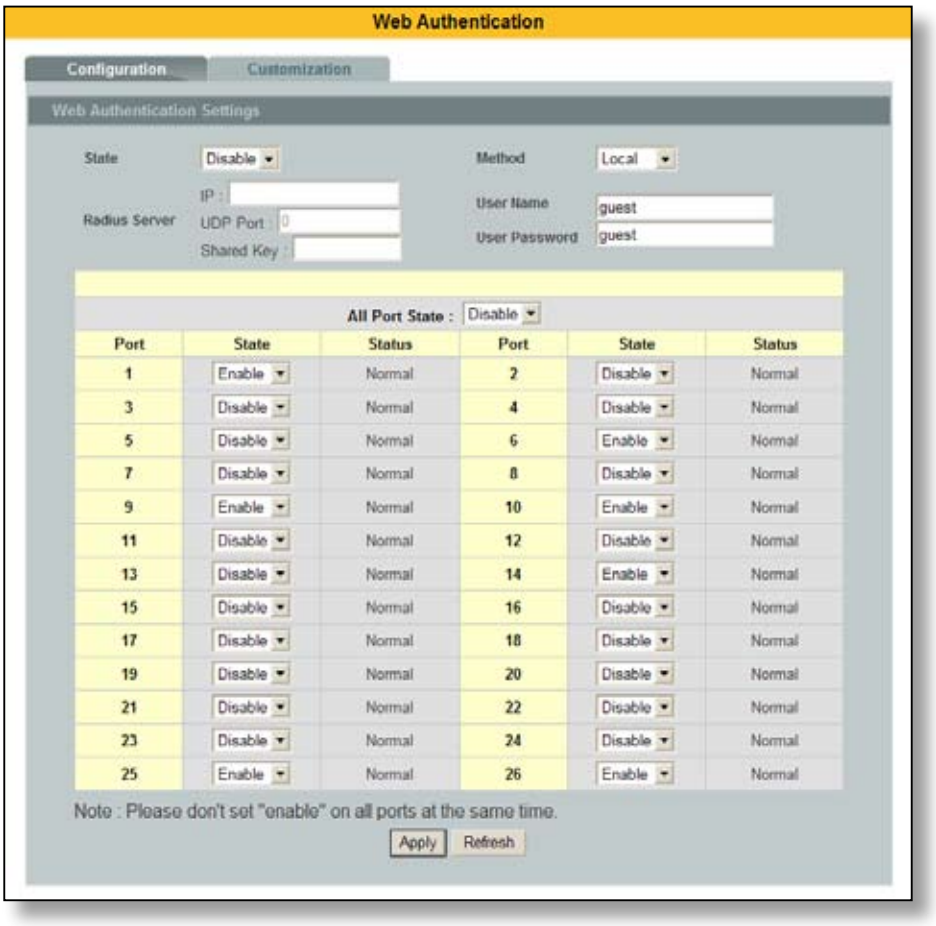
Web Authentication

Web authentication allows the admin to set a username and password for logins on a particular port. This is usually employed one guest terminals or networks, for example in a company meeting room, where guests can be allowed to connect to the internet. The administrator can choose to either enable RADIUS (in which case the authentication method will be controlled by a RADIUS server) or use the simple on-switch authentication service.

For a RADIUS server, fill out the three boxes for IP (the IP address of the RADIUS server), UDP port, and shared key.

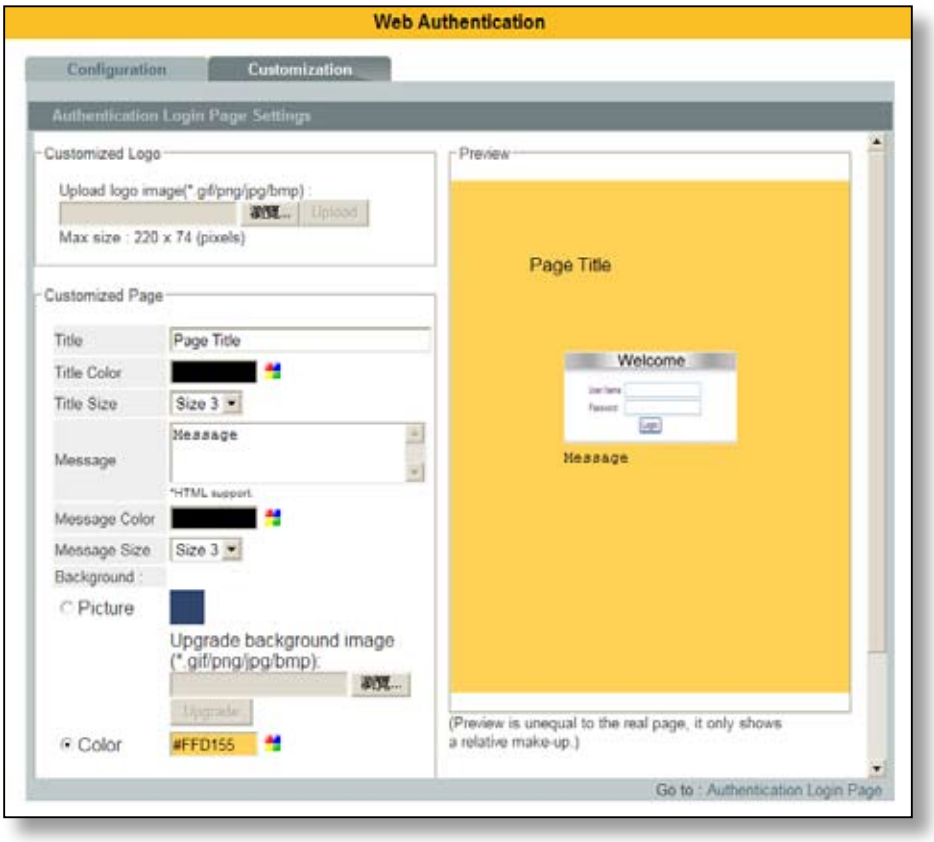
To set a username and password for switch-based authentication, enter the relevant username and password in the boxes on the right.

The administrator should select the ports for application of the web authentication below, then click **apply** to save.



The customization option allows the administrator to customize the web authentication login screen that users will see when they attempt to access the network. Administrators can change the colors, font sizes, and backgrounds, and also add a logo if required.

Once the desired changes have been made, click **preview** to see a small preview on the right hand side, or **apply** to save the settings.



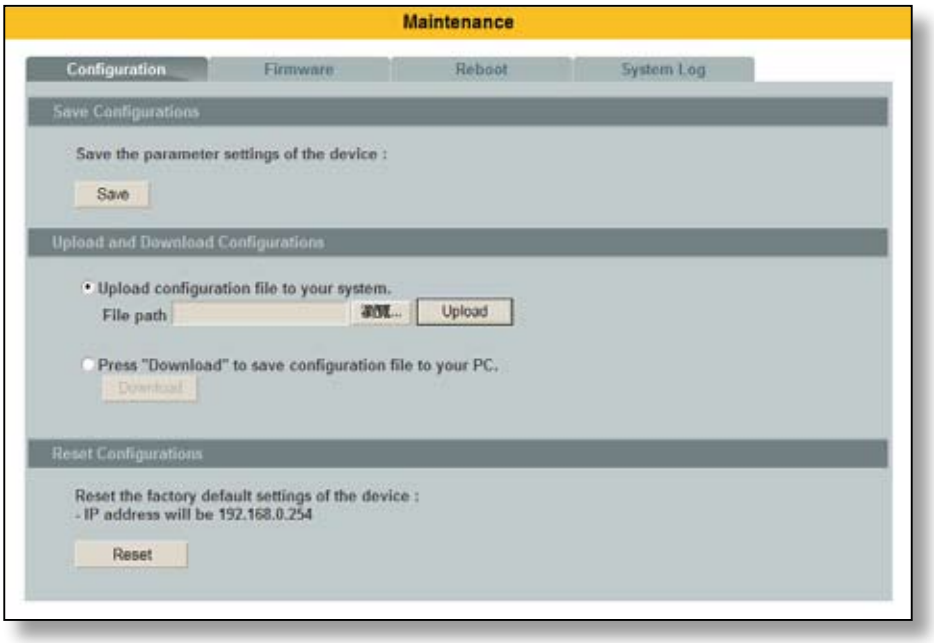
Management

The management section deals specifically with switch management.

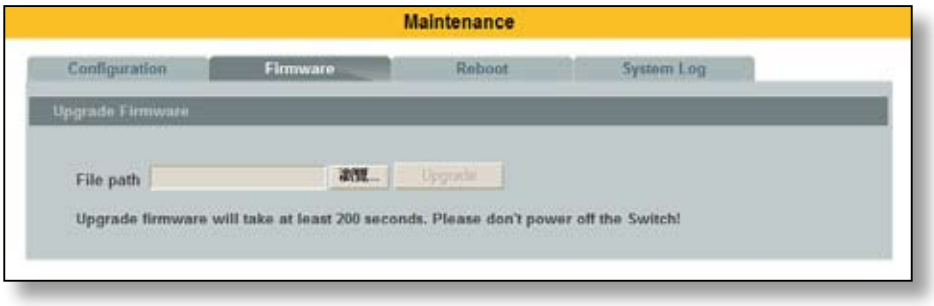
Maintenance

The configuration tab is used to save and restore settings to the device. The user can back up the switch settings to a PC to use as a later restore point using the **backup** button. To restore from a backup, click the browse button to locate the relevant backup file on a PC, then click apply to restore.

In order to restore the switch settings to the default, click **reset** in the Restore Default Factory Configuration section.

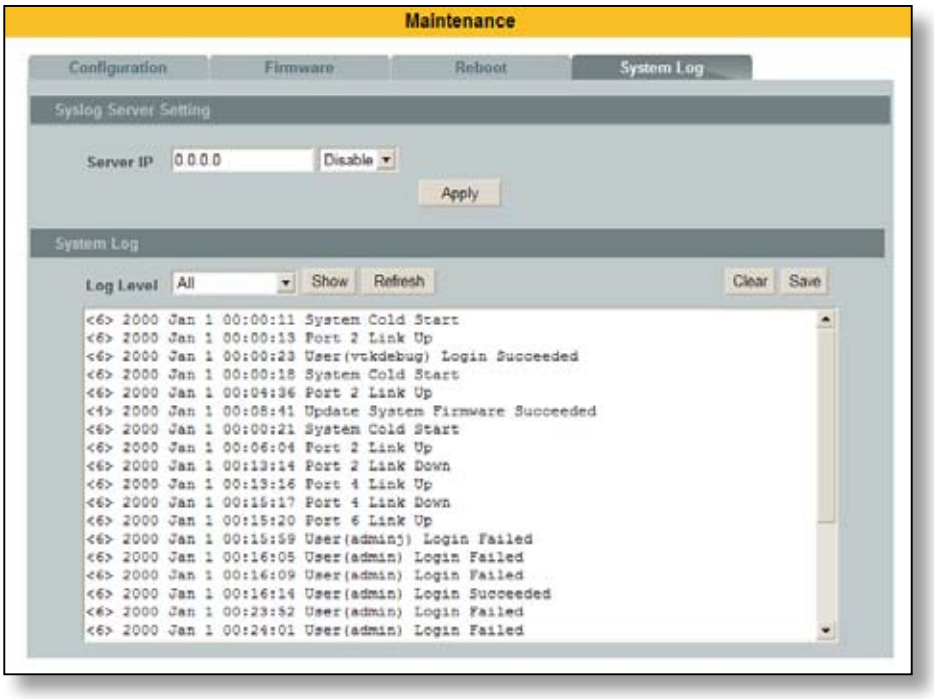


To upgrade the firmware, select the file path for the firmware file by using the browse button and locating the file on the computer's hard drive. Click upgrade to install the new firmware.



To reboot the switch, click the reboot tab and then click the reboot button. The switch will shut down and restart.

The system log details actions, inputs and messages generated by the switch. Click **refresh** to see the latest updates.

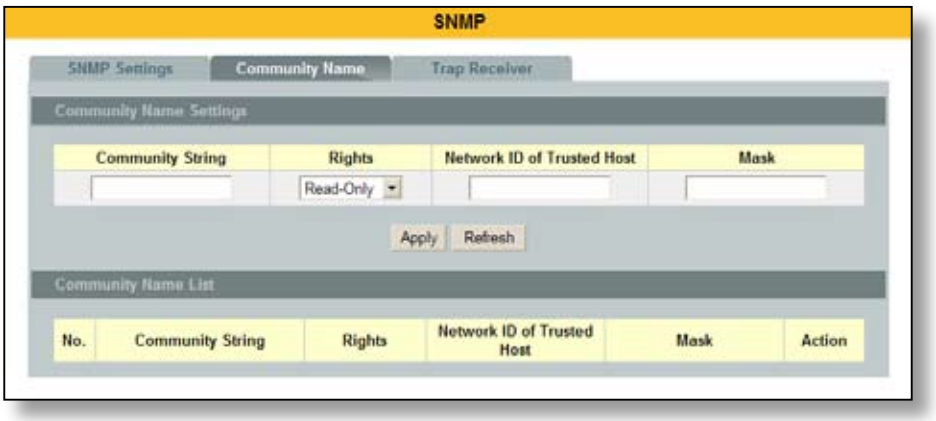


SNMP

Simple Network Management Protocol is a method of controlling the switch remotely through an external aggregation switch. This is usually used on larger networks, giving the administrator the power to control all switches in a network through one, higher security switch.

The SNMP settings window allows the network administrator to enter SNMP settings. Once the relevant details have been entered, click **apply** to save.

The community name tab is used to control community access to the switch management. Enter the community string, rights level, and trusted host IP to activate. Click apply to save.



The trap receiver tab is used to set an IP, version number and community string for trap reception. Enter the relevant details and click **apply** to save.

User Account

The User Account section is used to create new users and delete existing users. The network administrator must set the user name, user password, and user authority level (guest/user/admin). Once this information has been entered, click **apply** to save.